UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/994,878	12/19/1997	MICHAEL A. EPSTEIN	PHA-23.313	7153

7590 04/23/2002

JACK E HAKEN
US PHILIPS CORP
INTELLECTUAL PROP DEPT
580 WHITE PLAINS ROAD
TARRYTOWN, NY 10591

EXAMINER
SONG, HOSUK

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 04/23/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.	Applicant(s)
08/994,878	Epstein
Examiner	**Art Unit**
Ho S. Song	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *Jan 24, 2002*.

2a) ☐ This action is **FINAL.** 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1, 2, 5-8, 11-16, and 19* is/are pending in the application.

4a) Of the above, claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1, 2, 5-8, 11-16, and 19* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13) ☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a) ☐ All b) ☐ Some* c) ☐ None of:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

*See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

15) ☒ Notice of References Cited (PTO-892)

16) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

17) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s). _____

18) ☐ Interview Summary (PTO-413) Paper No(s). _____

19) ☐ Notice of Informal Patent Application (PTO-152)

20) ☐ Other:

DETAILED ACTION

1. Finality of last office action has been withdrawn.

2. The previous grounds of rejection based on Spies patent are withdrawn. However, newly discovered have necessitated new grounds of rejections. The delay in citation of the newly discovered prior art is regretted. The new grounds of rejections are presented below.

Claim Rejections - 35 USC § 103

3 The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4 Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable by Trostle(US 5,919,257) in view of Asay et al.(US 5,903,882).

In claim 5, Trostle teaches user transmitting ID over the network in (col.5, lines 50-51). Trostle discloses reading from a storage data corresponding to the user having the received ID, which data comprises the user's private key encrypted using a key determined from identifying information of the user and sending via network the encrypted private key, whereby the encrypted key can be received and decrypted at the location of the user's identifying information in (col.5, lines 51-57). Trostle does not discloses destroying any non-volatile record of the private key at the location of the user. Asay disclose in (col.30, lines 55-57 and col.55, lines 38-43) where after application is signed by a private key, private key is destroyed at the user's site. It would have been obvious to person of ordinary skill in the art at the time invention was made to destroy a

private key at the user's site taught in Asay with a public key system disclosed in Trostle in order to assure the user that private key is no longer available for access if attempted by the hackers and since private key is discarded at user's site, the user has total control of its key rather than key handled at the remote site where it can be viable for attacks.

In claim 7, the examiner takes official notice that hashing a document is well known in the art. The most common cryptographic uses of hash functions are with digital signatures and for data security. One of ordinary skill in the art would be motivated to use hash function in order to save both time and space.

5. Claims 6,8, are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle in view of Schneier and further in view of Asay.

In claims 6,8, Trostle discloses all the limitations above. However, Trostle does not discloses Passphrase scheme. Schneier discloses passphrase scheme in (page 174, passphrase section). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use passphrase taught in Schneier for password of Trostle so that user can remember phrases easier than random character sequences. Passphrase provides greater security through increased entropy than a short password. Trostle/Schneier does not disclose processing user's approval of the document. Asay's patent disclose digitally signing a user's approval document using a private key. It would have been obvious to person of ordinary skill in the art at the time invention was made to have approval/validation process done by the user as taught in Asay with validation process disclosed in Trostle so that if the system is idle or left unattended by the user

any intruders or hackers can compromise the system. Manual validation process such as digital signing of the document done by the user assures security. The examiner takes official notice that hashing a document is well known in the art. The most common cryptographic uses of hash functions are with digital signatures and for data security. One of ordinary skill in the art would be motivated to use hash function in order to save both time and space.

6. Claims 1,11,13,15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle in view of Asay (US 5,689,565).

In claim 1, Trostle discloses user transmitting ID over the network in (col.5, lines 50-51). Trostle discloses reading from a storage data corresponding to the user having the received ID, which data comprises the user's private key encrypted using a key determined from identifying information of the user and sending via network the encrypted private key, whereby the encrypted key can be received and decrypted at the location of the user's identifying information in (col.5, lines 51-57). However, Trostle does not specifically discloses public key corresponding to the private key. The examiner asserts that Trostle teaches asymmetric key system by user transmitting username over the network and remote server compares username against a list and transmits corresponding private key to the user. It would have been obvious to person of ordinary skill in the art to recognize that this is a public key system. One of ordinary skill in the art would be motivated to use public key scheme because it is faster and it provides better security than symmetric key system. Trostle does not teach encrypting or decrypting the hash value using the user's private key. The examiner takes official notice that hashing a document is well known

in the art. The most common cryptographic uses of hash functions are with digital signatures and for data security. One of ordinary skill in the art would be motivated to use hash function in order to save both time and space. Asay's patent disclose digitally signing a user's approval document using a private key. It would have been obvious to person of ordinary skill in the art at the time invention was made to have approval/validation process done by the user as taught in Asay with validation process disclosed in Trostle so that if the system is idle or left unattended by the user any intruders or hackers can compromise the system. Manual validation process such as digital signing of the document done by the specific user assures security.

In claims 11,13,15, Trostle discloses computer storage and a server in (fig.1). Trostle discloses storage including respective IDs and encrypted private keys for the respective users in which private keys have been encrypted using respective keys determined from respective user identifying information and server reading an encrypted private key from the storage with corresponding to a particular user and transmitting the encrypted private key to the particular user in (fig.5 and col.5, lines 49-57). Trostle does not teach encrypting or decrypting the hash value using the user's private key. The examiner takes official notice that hashing a document is well known in the art. The most common cryptographic uses of hash functions are with digital signatures and for data security. One of ordinary skill in the art would be motivated to use hash function in order to save both time and space. Asay's patent disclose digitally signing a user's approval document using a private key. It would have been obvious to person of ordinary skill in the art at the time invention was made to have approval/validation process done by the user as

taught in Asay with validation process disclosed in Trostle so that if the system is idle or left unattended by the user any intruders or hackers can compromise the system. Manual validation process such as digital signing of the document done by the specific user assures security.

7 Claims 2,6,12,14,16,19, are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle in view of Asay and further in view of Schneier.

In claims 2,6,12,19, Trostle discloses all the limitations above. However, Trostle does not discloses passphrase. Schneier discloses passphrase scheme in (page 174, passphrase section). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use passphrase taught in Schneier for password of Trostle so that user can remember phrases easier than random character sequences. Passphrase provides greater security through increased entropy than a short password. Asay disclose in (col.30, lines 55-57 and col.55, lines 38-43) where after application is signed by a private key, private key is destroyed at the user's site. It would have been obvious to person of ordinary skill in the art at the time invention was made to destroy a private key at the user's site taught in Asay with a public key system disclosed in Trostle in order to assure the user that private key is no longer available for access if attempted by the hackers and since private key is discarded at user's site, the user has total control of its key rather than key handled at the remote site where it can be viable for attacks.

In claims 14,16 the examiner asserts that storage means the respective public keys corresponding to the private keys for the respective users is well known public key scheme. One

of ordinary skill in the art would be motivated to use public key method because it is much secure than secret key scheme.

In claim 19, see claim rejection 11 and 12 above.

8. Any inquiry concerning this communication should be directed to Ho S. Song at telephone number (703)305-0042. The examiner can normally be reached on Monday through Friday from 6:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached at (703)305-9711.

Any inquiry of a general nature or relating to the status of this application or preceding should be directed to the group receptionist, whose telephone number is (703)305-3900.

Ho Song

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100